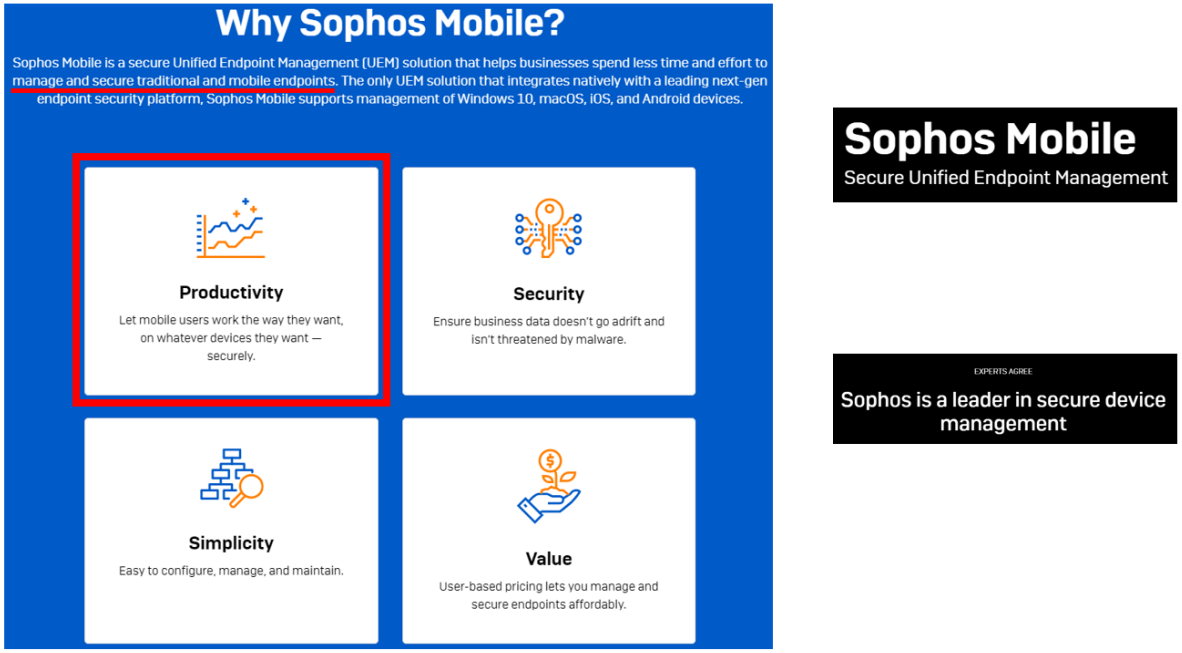
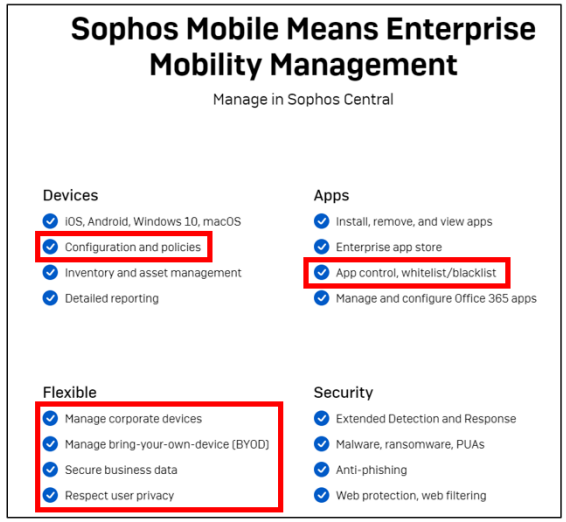
Exhibit 8

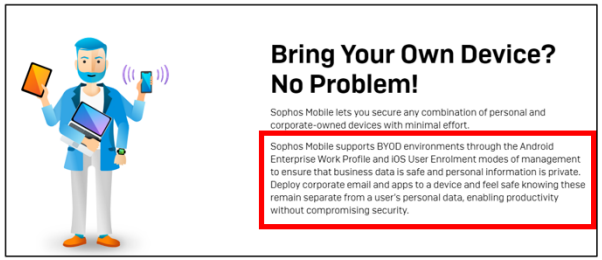
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
[1pre] A method of establishing plural modes of operation on a mobile device, the method comprising:	Sophos Mobile is an endpoint (e.g., mobile device) management tool  https://www.sophos.com/en-us/products/mobile-control

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

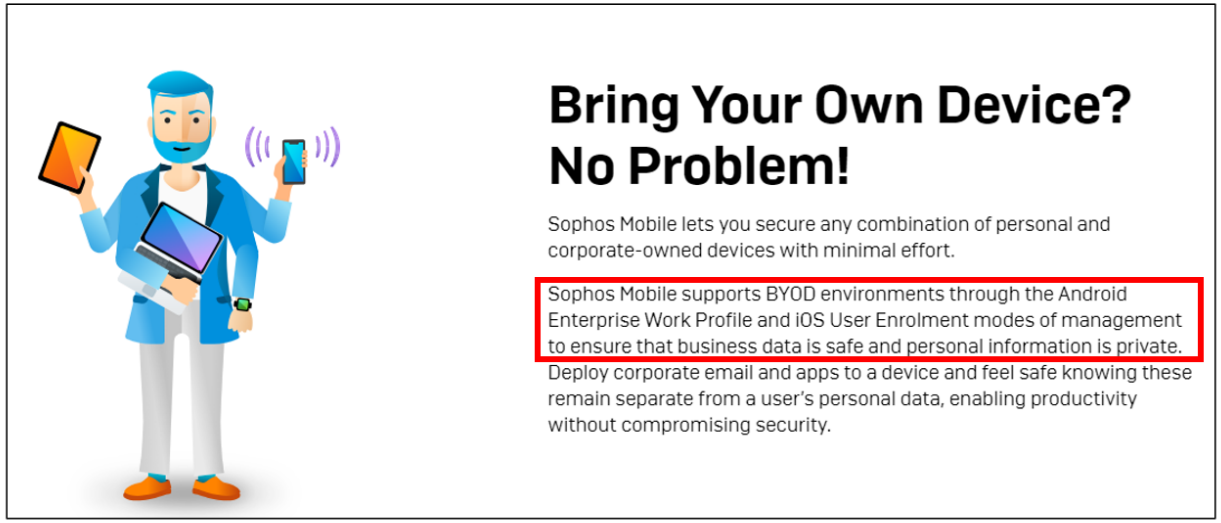
Claims	Identification
	Sophos Mobile supports BYOD environments through the management "mode" of Android (Android Enterprise Work Profile) to separate business and personal data. For example, corporate email and apps remain separate from personal data. It is possible to configure "policies" and establish "blacklist" and "whitelist" applications.



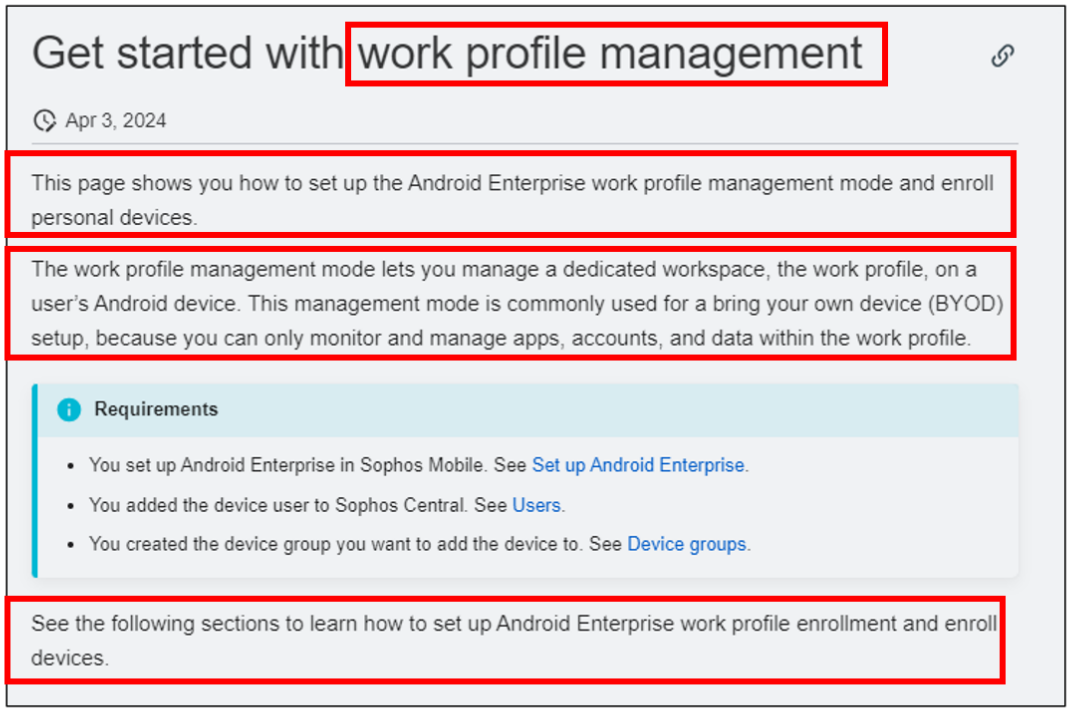


https://www.sophos.com/en-us/products/mobile-control

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

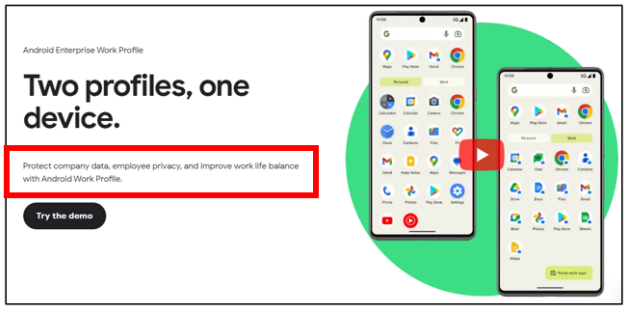
Claims	Identification
[1a] associating each application on the mobile device with one of a plurality of modes; and	Sophos Mobile supports the use of Android Enterprise Work Profile mode.  https://www.sophos.com/en-us/products/mobile-control

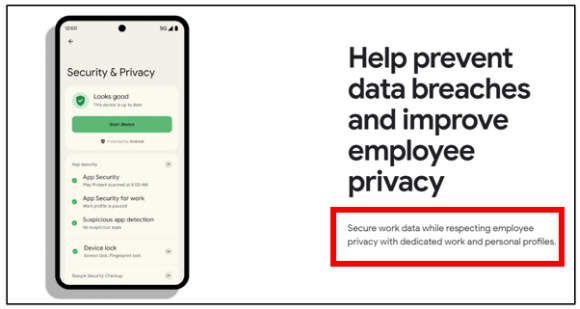
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

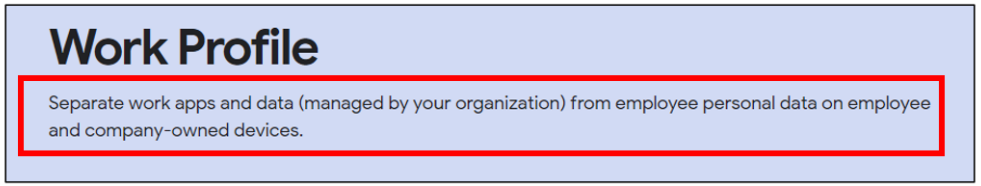
Claims	Identification
	Sophos Mobile supports the use of Android Enterprise Work Profile mode.  https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/EnrollDevices/AndroidEnterprise/WorkProfileGetStarted/index.html

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Sophos Mobile supports the use of Android Enterprise Work Profile mode, which separates "work" and "personal" apps and data.





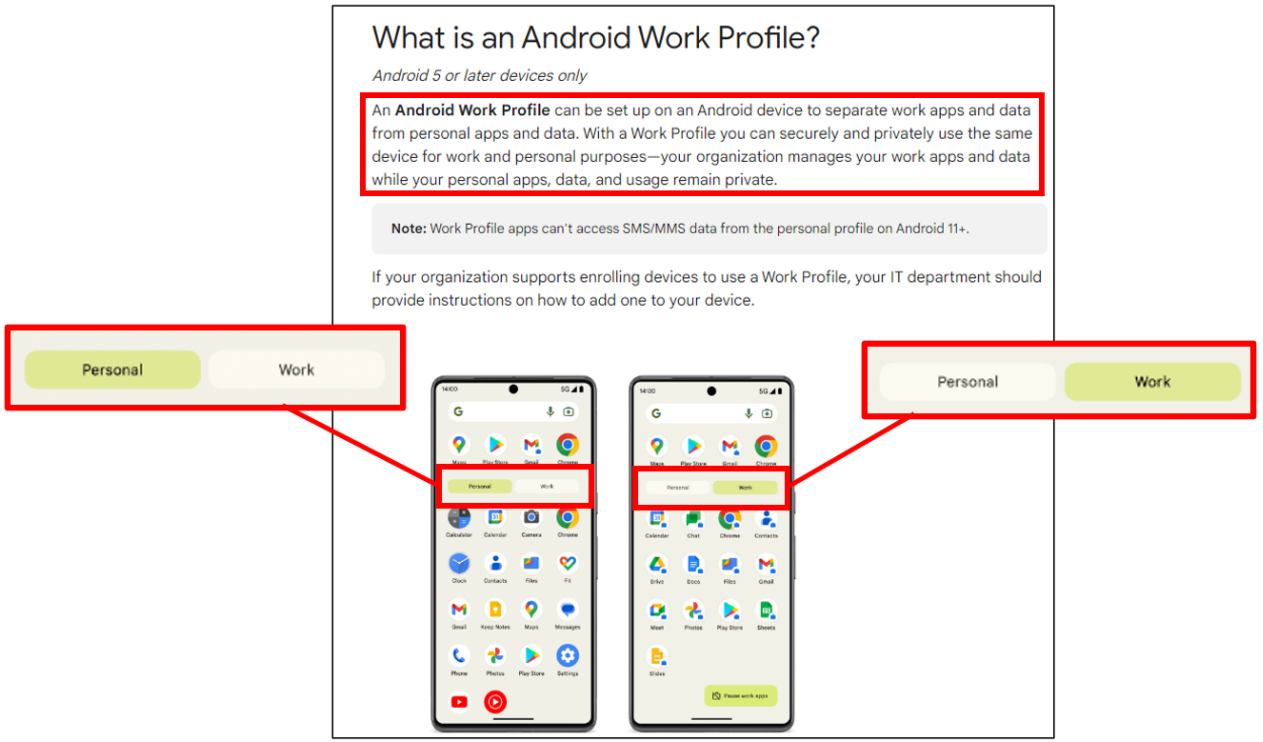


https://www.android.com/enterprise/work-profile/

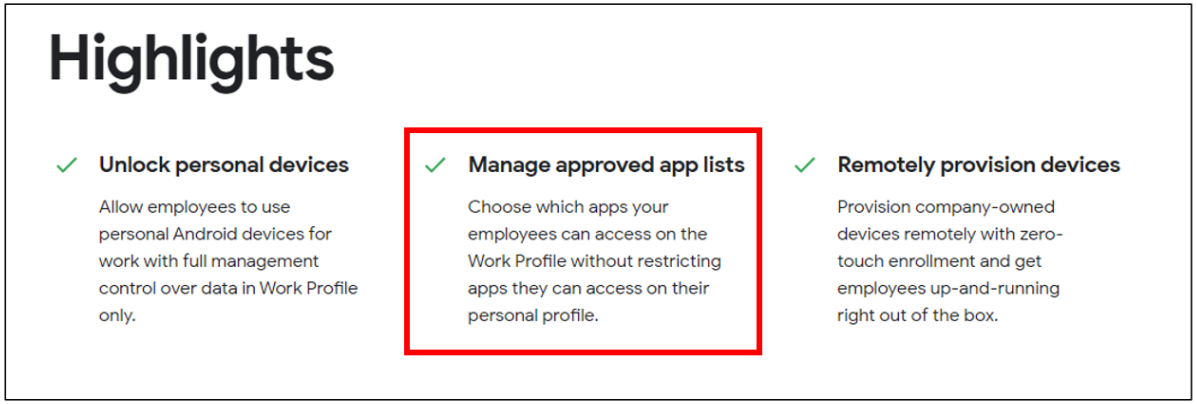
Claims	Identification
	In Android Enterprise Work Profile mode, "work" apps and data are associated with a work profile as separate from and "personal" apps and data. **Work Profile and its features** A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage. On devices designated as company-owned during setup, organizations can enforce some policies that apply to a device's personal profile and overall device behavior. Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see What is a Work Profile. https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features

Claims	Identification
	In Android Enterprise Work Profile mode, "work" apps and data are associated with a work profile as separate from and "personal" apps and data. **App management** EMM providers support Android app management through an enterprise version of Google Play, called managed Google Play. With an EMM, you can create Managed Google Play accounts* for your users. These accounts enable app distribution to their Work Profiles. **Feature** / **Description** View and manage your app catalog — View a list of purchased apps, approved apps, and private apps. Distribute apps silently — Silently install apps on a device without any user interaction. Download apps from the managed Play app — Users can install and update apps approved for them through the Managed Google Play app on their device. Set managed configurations — Configure work apps for individual users or devices. *For organizations with Google Workspace or Cloud Identity, users can access managed Google Play with their Google Workspace or Cloud Identity account. https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

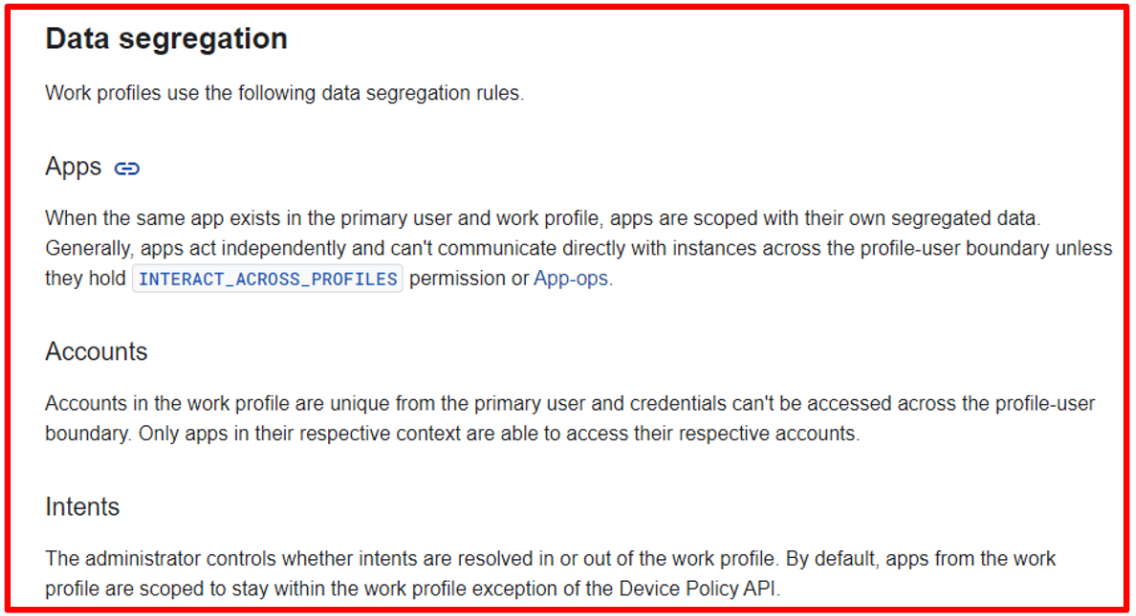
Claims	Identification
	In Android Enterprise Work Profile mode, "work" apps and data are associated with a work profile as separate from and "personal" apps and data.  https://support.google.com/work/android/answer/6191949?hl=en

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
[1b] restricting data on the mobile device to be accessible by only a subset of applications based on the mode associated with the application,	Android Enterprise Work Profile enables the creation of "approved app lists" that restricts data accessed by applications based on the mode.  https://www.android.com/enterprise/work-profile/

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile restricts data to be accessible based on the mode associated with the app, as apps are restricted to segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles.



Data segregation

Work profiles use the following data segregation rules.

Apps

When the same app exists in the primary user and work profile, apps are scoped with their own segregated data. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold `INTERACT_ACROSS_PROFILES` permission or App-ops.

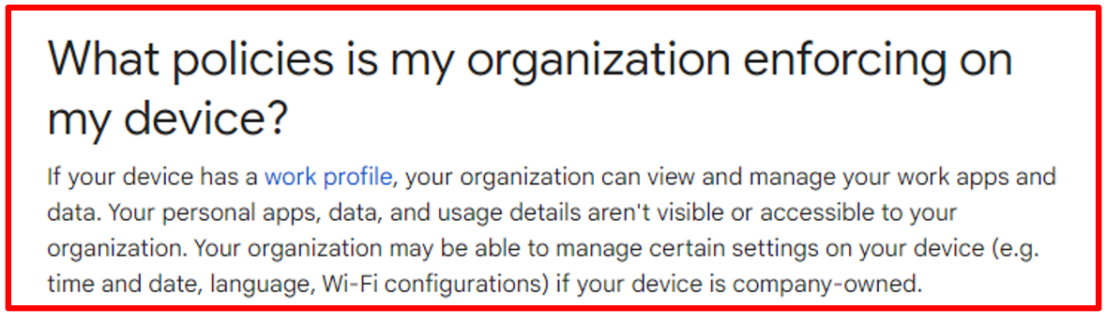
Accounts

Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts.

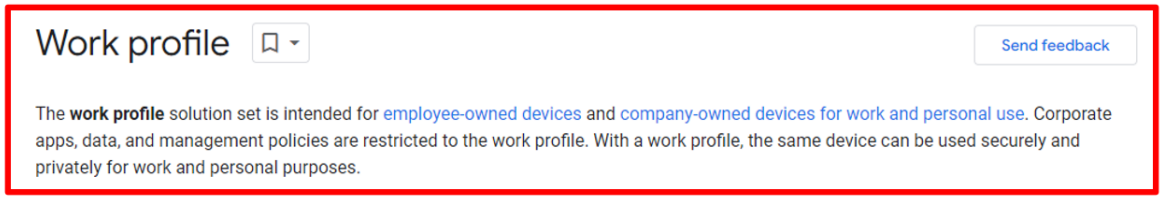
Intents

The administrator controls whether intents are resolved in or out of the work profile. By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API.

https://source.android.com/docs/devices/admin/managed-profiles

Claims	Identification
	Android Enterprise Work Profile enables the creation of "policies" that restrict data accessed by applications and control permissions based on the mode (e.g., "work" or "personal") associated with the app.  https://support.google.com/work/android/answer/7502354?sjid=4365723958134001885-NC

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile enables the creation of "policies" that restrict data accessed by applications and control permissions based on the mode (e.g., "work" or "personal") associated with the app.  https://developers.google.com/android/work/requirements/work-profile

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile enables the creation of "policies" that restrict data accessed by applications and control permissions based on the mode (e.g., "work" or "personal") associated with the app. Sophos Mobile provides a device policy controller app for implementing and managing Android Enterprise Work Profile. **What policies can my organization manage on my device?** When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile. If your device is personally-owned, your organization can carry out some or all of the following actions: • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization's corporate mail server and internal data • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device

Claims	Identification
	Android Enterprise Work Profile enables the creation of "policies" that restrict data accessed by applications and control permissions based on the mode (e.g., "work" or "personal") associated with the app.

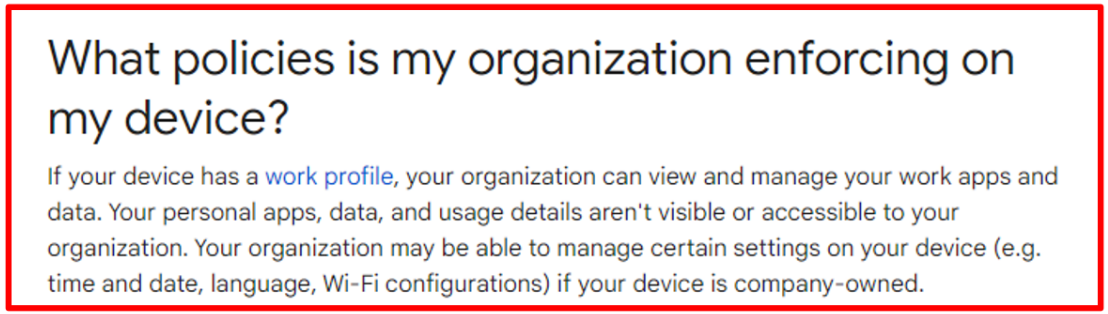
Device management

Feature	Description
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.

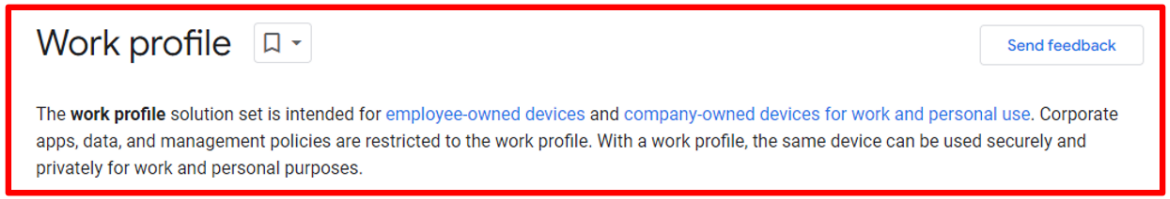
https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
[1c] wherein the data is associated with one of the plurality of modes and the restricting comprises adding a group permission to the data and providing each application with access to the data based on the group permission, the group permission for data associated with one of the plurality of modes controls access to the data by applications associated with the others of the plurality of modes, and	Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., "work" or "personal"), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the "work" or "personal" mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the "work" or "personal" mode), where the group permission for "work" mode controls access to "work" data by "personal" apps. **Data segregation** Work profiles use the following data segregation rules. Apps When the same app exists in the primary user and work profile, apps are scoped with their own segregated data. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold `INTERACT_ACROSS_PROFILES` permission or App-ops. Accounts Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts. Intents The administrator controls whether intents are resolved in or out of the work profile. By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API. https://source.android.com/docs/devices/admin/managed-profiles

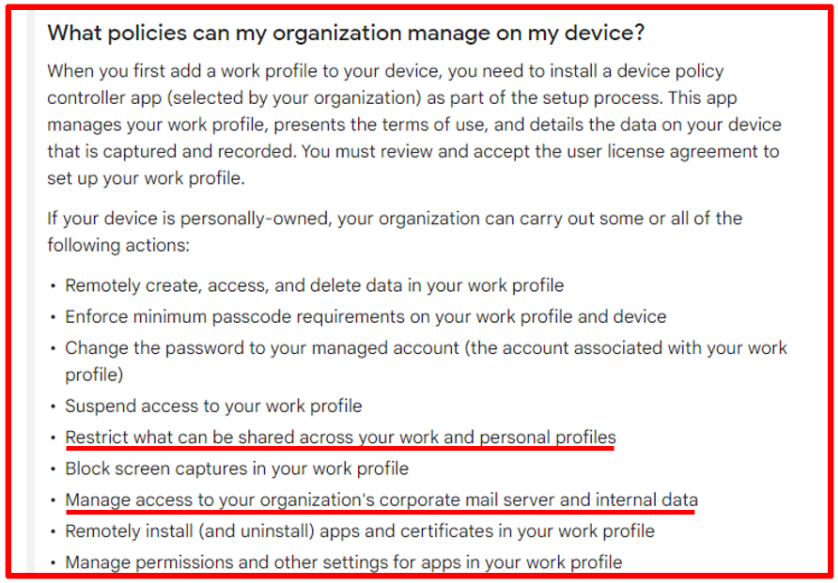
Claims	Identification
	Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., "work" or "personal"), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the "work" or "personal" mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the "work" or "personal" mode), where the group permission for "work" mode controls access to "work" data by "personal" apps.  What policies is my organization enforcing on my device? If your device has a work profile, your organization can view and manage your work apps and data. Your personal apps, data, and usage details aren't visible or accessible to your organization. Your organization may be able to manage certain settings on your device (e.g. time and date, language, Wi-Fi configurations) if your device is company-owned. https://support.google.com/work/android/answer/7502354?sjid=4365723958134001885-NC

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., "work" or "personal"), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the "work" or "personal" mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the "work" or "personal" mode), where the group permission for "work" mode controls access to "work" data by "personal" apps.  https://developers.google.com/android/work/requirements/work-profile

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., "work" or "personal"), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the "work" or "personal" mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the "work" or "personal" mode), where the group permission for "work" mode controls access to "work" data by "personal" apps.



What policies can my organization manage on my device?

When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.

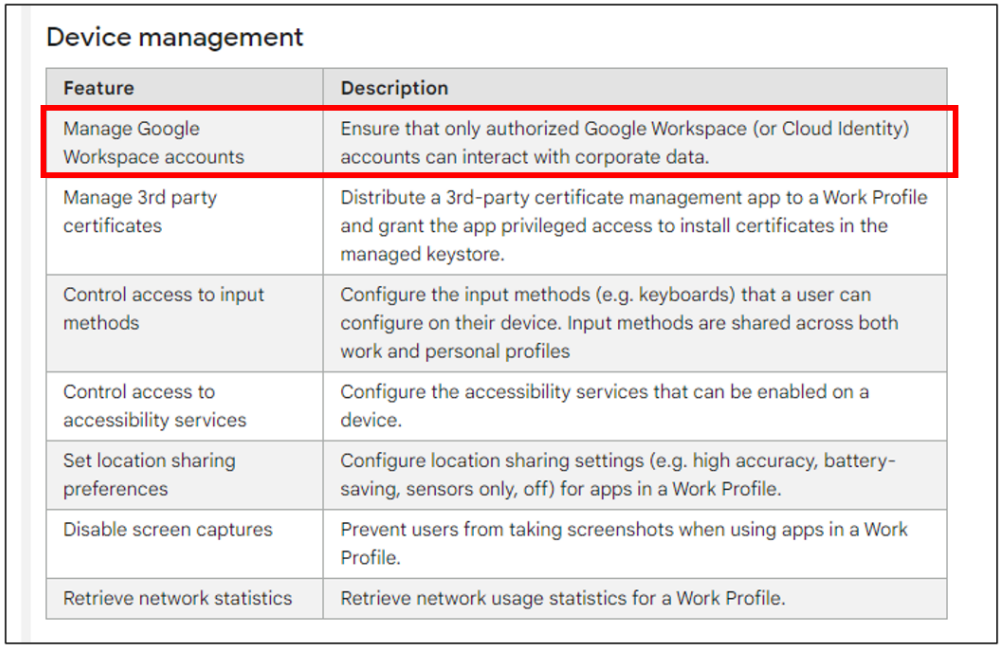
If your device is personally-owned, your organization can carry out some or all of the following actions:

- Remotely create, access, and delete data in your work profile
- Enforce minimum passcode requirements on your work profile and device
- Change the password to your managed account (the account associated with your work profile)
- Suspend access to your work profile
- Restrict what can be shared across your work and personal profiles
- Block screen captures in your work profile
- Manage access to your organization's corporate mail server and internal data
- Remotely install (and uninstall) apps and certificates in your work profile
- Manage permissions and other settings for apps in your work profile

https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., "work" or "personal"), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the "work" or "personal" mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the "work" or "personal" mode), where the group permission for "work" mode controls access to "work" data by "personal" apps.

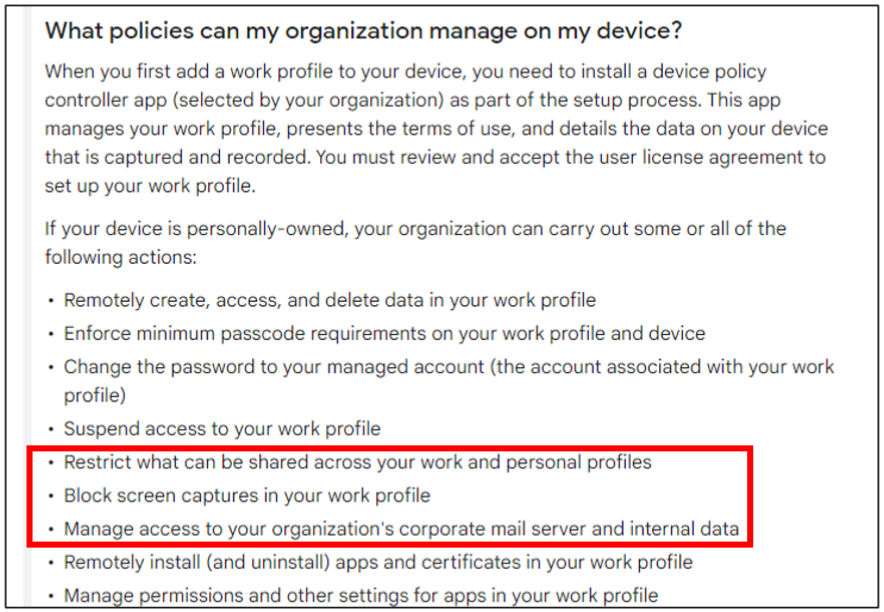


Device management

Feature	Description
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.

https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
[1d] the group permission for the data limits the ability to copy a subset of the data between modes, where some data can be copied directly between modes, and	Android Enterprise Work Profile polices can limit the ability to copy data between modes.  **What policies can my organization manage on my device?** When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile. If your device is personally-owned, your organization can carry out some or all of the following actions: • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization's corporate mail server and internal data • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile polices can limit the ability to copy data between modes.

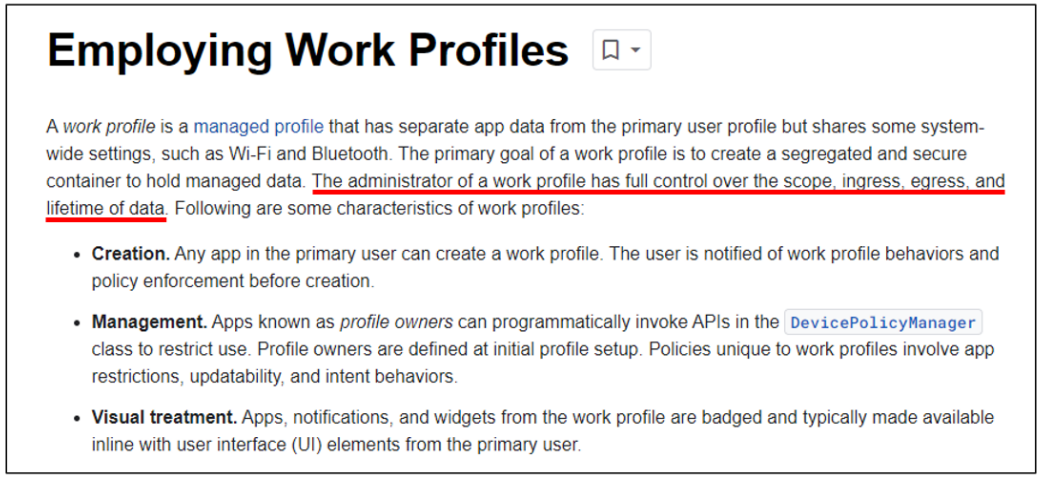
Device management

Feature	Description
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.

https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
[1e] wherein data associated with the first mode is deleted from the mobile device when such data is not accessed within a time period, while data associated with the second mode does not have a deletion policy.	Android Enterprise Work Profile allows work profile administrator to control the "lifetime" and "egress" of data.



Employing Work Profiles

A *work profile* is a managed profile that has separate app data from the primary user profile but shares some system-wide settings, such as Wi-Fi and Bluetooth. The primary goal of a work profile is to create a segregated and secure container to hold managed data. The administrator of a work profile has full control over the scope, ingress, egress, and lifetime of data. Following are some characteristics of work profiles:

- **Creation.** Any app in the primary user can create a work profile. The user is notified of work profile behaviors and policy enforcement before creation.
- **Management.** Apps known as *profile owners* can programmatically invoke APIs in the `DevicePolicyManager` class to restrict use. Profile owners are defined at initial profile setup. Policies unique to work profiles involve app restrictions, updatability, and intent behaviors.
- **Visual treatment.** Apps, notifications, and widgets from the work profile are badged and typically made available inline with user interface (UI) elements from the primary user.

https://source.android.com/docs/devices/admin/managed-profiles

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	Android Enterprise Work Profile allows work profile administrator to control the deletion of data. **What policies can my organization manage on my device?** When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile. If your device is personally-owned, your organization can carry out some or all of the following actions: • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization's corporate mail server and internal data • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device